

Serial Number 09/893,465

AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for protecting keys used to digitally sign files to be downloaded to a terminal, comprising:

a smartcard having stored thereon a private key; and

a file signing tool arranged to receive a file to be signed, to access the smartcard, and to download the file to the terminal,

wherein the smartcard includes an embedded secure processor programmed to perform all digital signing operations that require access to the private key before supplying results of the operations to the file signing tool, the file signing tool then performing further processing as necessary to generate a digital signature that is appended to the file for download to the terminal,

wherein said smartcard has stored thereon an authentication level indicating a number of PINs that must be input in order to access the smartcard.

2. (Original) A system as claimed in claim 1, wherein the smartcard also has stored thereon a signer certificate containing a public key corresponding to said private key.

3. (Original) A system as claimed in claim 2, wherein said file signer tool is arranged to retrieve said signer certificate from said smartcard and append the signer certificate to the signed file for use by the terminal in authenticating a digital signature generated by the smartcard and file signing tool.

4. (Original) A system as claimed in claim 3, wherein the signer certificate includes a field designating file types that may be authenticated by the signer certificate.

Serial Number 09/893,465

5. (Original) A system as claimed in claim 3, further comprising an owner certificate installed on said terminal for use by the terminal in authenticating the signer certificate.

6. (Original) A system as claimed in claim 1, wherein the smartcard also has stored thereon a PIN, and wherein said smartcard is arranged to perform digital signing operations only if a corresponding PIN is input through said file signing tool.

7. (Canceled)

8. (Original) A system as claimed in claim 7_1, wherein said PINs that must be input are combined by a logical exclusive OR operation in order to obtain a combined PIN to be compared with a PIN stored on the smartcard before said digital signing operations are performed.

9. (Original) A system as claimed in claim 7_1, wherein different ones of said PINs permit access to different private keys and public keys certificates having different file type properties, thereby enabling different authorization levels to be established.

10. (Currently Amended) A system for protecting keys used to digitally sign files to be downloaded to a terminal, comprising:

a smartcard; and

means for storing a private key on the smartcard and means for protecting the private key by requiring input of multiple PINs before the smartcard can be accessed,

wherein the smartcard includes an embedded secure processor programmed to perform all digital signing operations that require access to the private key,

wherein said PINs that must be input are combined in order to obtain a combined PIN to be compared with a PIN stored on the smartcard before said digital signing operations are performed.

11-18. (Canceled)

Serial Number 09/893,465

19. (Original) A method as claimed in claim 18, further of protecting keys used to digitally sign files to be downloaded to a terminal, comprising the steps of:

providing a smartcard having stored thereon a private key;

providing a file signing tool arranged to receive a file to be signed, to access the smartcard, and to download the file to the terminal;

storing at least one PIN on the smartcard;

storing an authentication level on the smartcard, said authentication level indicating a number of PINs that must be input to the file signing tool in order to enable said file signing tool to access the smartcard;

reading the authentication level and prompting at least one user to input said PINs to the file signing tool;

combining said PINs to obtain a combined PIN; and

comparing said combined PIN with said at least one PIN stored on the smartcard before said digital signing operations are performed; and

if said combined PIN corresponds to said at least one PIN stored on the smartcard, utilizing a secure processor embedded in the smartcard to perform all digital signing operations that require access to the private key before supplying results of the operations to the file signing tool, the file signing tool then performing further processing as necessary to generate a digital signature that is appended to the file for download to the terminal.

20. (Original) A method as claimed in claim 18, further comprising the step of storing on said smartcard a plurality of said PINs in order to permit access to different private keys and public keys certificates having different file type properties, thereby enabling different authorization levels to be established.

21. (New) A system as claimed in claim 10, wherein said PINs that must be input are combined by a logical exclusive OR operation in order to obtain said combined PIN.

Serial Number 09/893,465

22. (New) A system as claimed in claim 10, wherein different ones of said PINs permit access to different private keys and public keys certificates having different file type properties, thereby enabling different authorization levels to be established.